A structure theorem for product sets in extra special groups

Thang Pham* Michael Tait† Le Anh Vinh‡ Robert Won§

Abstract

Hegyvári and Hennecart showed that if B is a sufficiently large brick of a Heisenberg group, then the product set $B \cdot B$ contains many cosets of the center of the group. We give a new, robust proof of this theorem that extends to all extra special groups as well as to a large family of quasigroups.

1 Introduction

Let p be a prime. An extra special group G is a p-group whose center Z is cyclic of order p such that G/Z is an elementary abelian p-group (nice treatments of extra special groups can be found in [2, 6]). The extra special groups have order p^{2n+1} for some $n \geq 1$ and occur in two families. Denote by H_n and M_n the two non-isomorphic extra special groups of order p^{2n+1}. Presentations for these groups are given in [4]:

$$\begin{aligned} H_n = \langle a_1, b_1, \ldots, a_n, b_n, c \mid & [a_i, a_j] = [b_i, b_j] = 1, [a_i, b_j] = 1 \text{ for } i \neq j, \\ & [a_i, c] = [b_i, c] = 1, [a_i, b_i] = c, a_i^p = b_i^p = c_i^p = 1 \text{ for } 1 \leq i \leq n\rangle \\ M_n = \langle a_1, b_1, \ldots, a_n, b_n, c \mid & [a_i, a_j] = [b_i, b_j] = 1, [a_i, b_j] = 1 \text{ for } i \neq j, \\ & [a_i, c] = [b_i, c] = 1, [a_i, b_i] = c, a_i^p = c_i^p = 1, b_i^p = c \text{ for } 1 \leq i \leq n\rangle. \end{aligned}$$

From these presentations, it is not hard to see that the center of each of these groups consists of the powers of c so are cyclic of order p. It is also clear that the quotient of both groups by their centers yield elementary abelian p-groups.

In this paper we consider the structure of products of subsets of extra special groups. The structure of sum or product sets of groups and other algebraic structures has a rich history in combinatorial number theory. One seminal result is Freiman's theorem [5], which asserts that if A is a subset of integers and $|A + A| = O(|A|)$, then A must be a subset of a small generalized arithmetic progression. Green and Ruzsa [7] showed that the same result is true in any abelian group. On the other hand, commutativity is important as the theorem is not true for general non-abelian groups [8]. With this in mind, Hegyvári and Hennecart were motivated to study what actually can be said about the structure of product sets in non-abelian groups. They proved the following theorem.

*Department of Mathematics, EPFL, Lausanne, Switzerland. Email thang.pham@epfl.ch

†Department of Mathematical Sciences, Carnegie Mellon University. Research is supported by NSF grant DMS-1606350. Email: mtait@cmu.edu.

‡University of Education, Vietnam National University. Email: vinhla@vnu.edu.vn

§Department of Mathematics, Wake Forest University. Email: wonrj@wfu.edu

Theorem 1.1 (Hegyvári-Hennecart, [9]). *For every $\varepsilon > 0$, there exists a positive integer n_0 such that if $n \geq n_0$, $B \subseteq H_n$ is a brick and*

$$|B| > |H_n|^{3/4+\varepsilon}$$

then there exists a non trivial subgroup G' of H_n, namely its center $[\underline{0}, \underline{0}, \mathbb{F}_p]$, such that $B \cdot B$ contains at least $|B|/p$ cosets of G'.

The group H_1 is the classical Heisenberg group, so the groups H_n form natural generalizations of the Heisenberg group. Our main focus is on the second family of extra special groups M_n. The group H_n has a well-known representation as a subgroup of $\mathrm{GL}_{n+2}(\mathbb{F}_p)$ consisting of upper triangular matrices

$$[\underline{x}, \underline{y}, z] := \begin{bmatrix} 1 & \underline{x} & z \\ 0 & I_n & \underline{y} \\ 0 & 0 & 1 \end{bmatrix}$$

where $\underline{x}, \underline{y} \in \mathbb{F}_p^n$, $z \in \mathbb{F}_p$, and I_n is the $n \times n$ identity matrix. Let $\underline{e_i} \in \mathbb{F}_p^n$ be the i^{th} standard basis vector. In the presentation for H_n, a_i corresponds to $[\underline{e_i}, 0, 0]$, b_i corresponds to $[0, \underline{e_i}, 0]$ and c corresponds to $[0, 0, 1]$. By matrix multiplication, we have

$$[\underline{x}, \underline{y}, z] \cdot [\underline{x}', \underline{y}', z'] = [\underline{x} + \underline{x}', \underline{y} + \underline{y}', z + z' + \langle \underline{x}, \underline{y}' \rangle]$$

where $\langle \, , \rangle$ denotes the usual dot product.

A second focus of this paper is to consider generalizations of the higher dimensional Heisenberg groups where entries come from a quasifield Q rather than $\mathbb{F}_p$. We recall the definition of a quasifield:

A set L with a binary operation $*$ is called a *loop* if

1. the equation $a * x = b$ has a unique solution in x for every $a, b \in L$,
2. the equation $y * a = b$ has a unique solution in y for every $a, b \in L$, and
3. there is an element $e \in L$ such that $e * x = x * e = x$ for all $x \in L$.

A *(left) quasifield* Q is a set with two binary operations $+$ and $*$ such that $(Q, +)$ is a group with additive identity 0, $(Q^*, *)$ is a loop where $Q^* = Q \backslash \{0\}$, and the following three conditions hold:

1. $a * (b + c) = a * b + a * c$ for all $a, b, c \in Q$,
2. $0 * x = 0$ for all $x \in Q$, and
3. the equation $a * x = b * x + c$ has exactly one solution for every $a, b, c \in Q$ with $a \neq b$.

Given a quasifield Q, we define $H_n(Q)$ by the set of elements

$$\{[\underline{x}, \underline{y}, z] : \underline{x} \in Q^n, \underline{y} \in Q^n, z \in Q\}$$

and a multiplication operation defined by

$$[\underline{x}, \underline{y}, z] \cdot [\underline{x}', \underline{y}', z'] = [\underline{x} + \underline{x}', \underline{y} + \underline{y}', z + z' + \langle \underline{x}, \underline{y}' \rangle].$$

Then $H_n(Q)$ is a quasigroup with an identity element (ie, a loop), and when $Q = \mathbb{F}_p$ we have that $H_n(Q)$ is the n-dimensional Heisenberg group H_n.

1.1 Statement of main results

Let H_n be a Heisenberg group. A subset B of H_n is said to be a *brick* if

$$B = \{[\underline{x}, \underline{y}, z] \text{ such that } \underline{x} \in \underline{X},\ \underline{y} \in \underline{Y},\ z \in Z\}$$

where $\underline{X} = X_1 \times \cdots \times X_n$ and $\underline{Y} = Y_1 \times \cdots \times Y_n$ with non empty-subsets $X_i, Y_i, Z \subseteq \mathbb{F}_p$.

Our theorems are analogs of Hegyvári and Hennecart's theorem for the groups M_n and the quasigroups $H_n(Q)$. In particular, their structure result is true for all extra special groups. We will define what it means for a subset B of M_n to be a brick in Section 2.1.

Theorem 1.2. *For every $\varepsilon > 0$, there exists a positive integer $n_0 = n_0(\varepsilon)$ such that if $n \geq n_0$, $B \subseteq M_n$ is a brick and*

$$|B| > |M_n|^{3/4+\varepsilon}$$

then there exists a non trivial subgroup G' of M_n, namely its center, such that $B \cdot B$ contains at least $|B|/p$ cosets of G'.

Combining Theorem 1.1 and Theorem 1.2, we have

Theorem 1.3. *Let G be an extra special group. For every $\varepsilon > 0$, there exists a positive integer $n_0 = n_0(\epsilon)$ such that if $n \geq n_0$, $B \subseteq G$ is a brick and*

$$|B| > |G|^{3/4+\varepsilon}$$

then there exists a non trivial subgroup G' of G, namely its center, such that $B \cdot B$ contains at least $|B|/p$ cosets of G'.

For Q a finite quasifield, we similarly define a subset $B \subseteq H_n(Q)$ to be a *brick* if

$$B = \{[\underline{x}, \underline{y}, z] \text{ such that } \underline{x} \in \underline{X},\ \underline{y} \in \underline{Y},\ z \in Z\}$$

where $\underline{X} = X_1 \times \cdots \times X_n$ and $\underline{Y} = Y_1 \times \cdots \times Y_n$ with non empty-subsets $X_i, Y_i, Z \subseteq Q$.

Theorem 1.4. *Let Q be a finite quasifield of order q. For every $\varepsilon > 0$, there exists an $n_0 = n_0(\varepsilon)$ such that if $n \geq n_0$, $B \subseteq H_n(Q)$ is a brick, and*

$$|B| > |H_n(Q)|^{3/4+\varepsilon},$$

then there exists a non trivial subquasigroup G' of $H_n(Q)$, namely its center $[\underline{0}, \underline{0}, Q]$ such that $B \cdot B$ contains at least $|B|/q$ cosets of G'.

Taking $Q = \mathbb{F}_p$ gives Theorem 1.1 as a corollary.

2 Preliminaries

2.1 A description of M_n

We give a description of M_n with which it is convenient to work. Define a group G whose elements are triples $[\underline{x}, \underline{y}, z]$ where $\underline{x} = (x_1, \ldots, x_n)$, $\underline{y} = (y_1, \ldots, y_n)$, with $x_i, y_i, z \in \mathbb{F}_p$ for $1 \leq i \leq n$. The group operation in G is given by

$$[\underline{x}, \underline{y}, z] \cdot [\underline{x}', \underline{y}', z'] = [\underline{x} + \underline{x}', \underline{y} + \underline{y}', z + z' + \langle \underline{x}, \underline{y}' \rangle + f(\underline{y}, \underline{y}')]$$

where the function $f : \mathbb{Z}^n \times \mathbb{Z}^n \to \mathbb{N}$ is defined by

$$f\left((y_1, \dots, y_n), (y'_1, \dots, y'_n)\right) = \sum_{i=1}^{n} \left\lfloor \frac{y_i \bmod p + y'_i \bmod p}{p} \right\rfloor.$$

Concretely, f counts the number of components where (after reducing mod p) $y_i + y'_i \geq p$. This is slight abuse of notation, as $\underline{y}, \underline{y}' \in \mathbb{F}_p^n$, but is well-defined if we regard them as elements of $\mathbb{Z}^n$.

Lemma 2.1. *With the operation defined above, G is a group isomorphic to M_n.*

Proof. We first need to check associativity of the operation. After cancellation, this reduces to checking the equality

$$f(\underline{y} + \underline{y}', \underline{y}'') + f(\underline{y}, \underline{y}') = f(\underline{y}, \underline{y}' + \underline{y}'') + f(\underline{y}', \underline{y}'')$$

which holds because

$$\begin{aligned} &\left\lfloor \frac{(y_i + y'_i) \bmod p + y_i \bmod p}{p} \right\rfloor + \left\lfloor \frac{y_i \bmod p + y'_i \bmod p}{p} \right\rfloor \\ &= \left\lfloor \frac{y_i \bmod p + y'_i \bmod p + y''_i \bmod p}{p} \right\rfloor \\ &= \left\lfloor \frac{(y_i + y'_i) \bmod p + y_i \bmod p}{p} \right\rfloor + \left\lfloor \frac{(y_i + y'_i) \bmod p + y_i \bmod p}{p} \right\rfloor, \end{aligned}$$

as all three of the expressions count the largest multiple of p dividing

$$y_i \bmod p + y'_i \bmod p + y''_i \bmod p.$$

Since G is generated $\{[\underline{e_i}, 0, 0], [0, \underline{e_i}, 0], [0, 0, 1]\}$, we define a homomorphism $\varphi : G \to M_n$ by $\varphi\left([\underline{e_i}, 0, 0]\right) = a_i$, $\varphi\left([0, \underline{e_i}, 0]\right) = b_i$, and $\varphi\left([0, 0, 1]\right) = c$. This map is clearly surjective and it is easy to check that the generators of G satisfy the relations in M_n. Since $|G| = p^{2n+1}$, φ is an isomorphism and $G \cong M_n$, as claimed. □

With this description, there is a natural way to define a brick in M_n. A subset B of M_n is said to be a *brick* if

$$B = \{[\underline{x}, \underline{y}, z] \text{ such that } \underline{x} \in \underline{X},\ \underline{y} \in \underline{Y},\ z \in Z\}$$

where $\underline{X} = X_1 \times \cdots \times X_n$ and $\underline{Y} = Y_1 \times \cdots \times Y_n$ with non empty-subsets $X_i, Y_i, Z \subseteq \mathbb{F}_p$.

2.2 Tools from spectral graph theory

For a graph G with vertex set $\{v_1, \dots, v_n\}$, the *adjacency matrix* of G is the matrix with a 1 in row i and column j if $v_i \sim v_j$ and a 0 otherwise. Since this is a real, symmetric matrix, it has a full set of real eigenvalues. Let $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_n$ be the eigenvalues of its adjacency matrix.

If G is a d-regular graph, then its adjacency matrix has row sum d. In this case, $\lambda_1 = d$ with the all-one eigenvector $\mathbf{1}$. Let $\mathbf{v}_i$ denote the corresponding eigenvector for λ_i. We will make use of the trick that for $i \geq 2$, $\mathbf{v}_i \in \mathbf{1}^{\perp}$, so $J\mathbf{v}_i = 0$ where J is the all-one matrix of size $n \times n$ (see [3] for more background on spectral graph theory).

It is well-known (see [1, Chapter 9] for more details) that if λ_2 is much smaller than the degree d, then G has certain random-like properties. A graph is called *bipartite* if its vertex set can be partitioned into two parts such that all edges have one endpoint in each part. For G be a bipartite graph with partite sets P_1 and P_2 and $U \subseteq P_1$ and $W \subseteq P_2$, let $e(U, W)$ be the number of pairs (u, w) such that $u \in U$, $w \in W$, and (u, w) is an edge of G. We recall the following well-known fact (see, for example, [1]).

Lemma 2.2 (Corollary 9.2.5, [1])**.** *Let $G = (V, E)$ be d-regular bipartite graph on $2n$ vertices with partite sets P_1 and P_2. For any two sets $B \subseteq P_1$ and $C \subseteq P_2$, we have*

$$\left| e(B, C) - \frac{d|B||C|}{n} \right| \leq \lambda_2 \sqrt{|B||C|}.$$

2.3 Sum-product graphs

Let Q be a finite quasifield. The sum-product graph $SP_{Q,n}$ is defined as follows. $SP_{Q,n}$ is a bipartite graph with its vertex set partitioned into partite sets $\mathbf{X}$ and $\mathbf{Y}$, where $\mathbf{X} = \mathbf{Y} = Q^n \times Q$. Two vertices $U = (\underline{x}, z) \in \mathbf{X}$ and $V = (\underline{y}, z') \in \mathbf{Y}$ are connected by an edge, $(U, V) \in E(SP_{Q,n})$, if and only if $\langle \underline{x}, \underline{y} \rangle = z + z'$. We need information about the eigenvalues of $SP_{Q,n}$.

Lemma 2.3. *If Q is a quasifield of order q, then the graph $SP_{Q,n}$ is q^n regular and has $\lambda_2 \leq 2^{1/2} q^{n/2}$.*

We provide a proof of Lemma 2.3 for completeness in the appendix, and we note that similar lemmas were proved in [11] and [10].

3 Proof of Theorem 1.2

Lemma 3.1. *Let $B \subseteq M_n$ be a brick in M_n with $B = [\underline{X}, \underline{Y}, Z]$ where $\underline{X} = X_1 \times \cdot \times X_n$ and $\underline{Y} = Y_1 \times \cdots \times Y_n$. For given $\underline{a} = (a_1, \ldots, a_n), \underline{b} = (b_1, \ldots, b_n) \in \mathbb{F}_p^n$, suppose that*

$$|Z|^2 \prod_{i=1}^{n} |X_i \cap (a_i - X_i)||Y_i \cap (b_i - Y_i)| > 2p^{n+2},$$

then we have

$$B \cdot B \supseteq [\underline{a}, \underline{b}, \mathbb{F}_p].$$

Proof. Let $X_i' = X_i \cap (a_i - X_i)$, $Y_i' = Y_i \cap (b_i - Y_i)$, $X' = (X_1', \ldots, X_n')$, and $Y' = (Y_1', \ldots, Y_n')$. We first have

$$B \cdot B \supseteq \{[\underline{x}, \underline{y}, z] \cdot [\underline{a} - \underline{x}, \underline{b} - \underline{y}, z'] : \underline{x} \in X', \underline{y} \in Y', z, z' \in Z\}.$$

On the other hand, it follows from the multiplicative rule in M_n that for

$$[\underline{x}, \underline{y}, z] \cdot [\underline{a} - \underline{x}, \underline{b} - \underline{y}, z'] = [\underline{a}, \underline{b}, z + z' + \langle \underline{x}, (\underline{b} - \underline{y}) \rangle + f(\underline{y}, \underline{b} - \underline{y})].$$

To conclude the proof of the lemma, it is enough to prove that

$$\left\{ z + z' + \langle \underline{x}, (\underline{b} - \underline{y}) \rangle + f(\underline{y}, \underline{b} - \underline{y}) \colon z, z' \in Z, \underline{x} \in X', \underline{y} \in Y' \right\} = \mathbb{F}_p$$

under the condition $|Z|^2|X'||Y'| > 2p^{n+2}$.

To prove this claim, let λ be an arbitrary element in $\mathbb{F}_p$, we define two sets in the sum-product graph $SP_{\mathbb{F}_p,n}$, $E \subseteq \mathbf{X}$ and $F \subseteq \mathbf{Y}$ as follows:

$$E = X' \times (-Z + \lambda),\ F = \left\{(\underline{b} - \underline{y}, -z - f(\underline{y}, \underline{b} - \underline{y}))\colon z \in Z, \underline{y} \in Y'\right\}.$$

It is clear that $|E| = |Z||X'|$ and $|F| = |Z||Y'|$. It follows from Lemma 2.2 and Lemma 2.3 that if $|Z|^2|X'||Y'| > 2p^{n+2}$, then $e(E, F) > 0$. It follows that there exist $\underline{x} \in X', \underline{y} \in Y'$, and $z, z' \in Z$ such that

$$z + z' + \langle \underline{x}, (\underline{b} - \underline{y})\rangle + f(\underline{y}, \underline{b} - \underline{y}) = \lambda.$$

Since λ is chosen arbitrarily, we have

$$\left\{z + z' + \langle \underline{x}, (\underline{b} - \underline{y})\rangle + f(\underline{y}, \underline{b} - \underline{y})\colon z, z' \in Z, \underline{x} \in X', \underline{y} \in Y'\right\} = \mathbb{F}_p. \qquad \square$$

Proof of Theorem 1.2. We follow the method of [9, Theorem 1.3]. First we note that if $|Z| > p/2$, then we have $Z + Z = \mathbb{F}_p$. This implies that

$$B \cdot B = [2\underline{X}, 2\underline{Y}, \mathbb{F}_p].$$

Therefore, $B \cdot B$ contains at least $|B \cdot B|/p \geq |B|/p$ cosets of the subgroup $[\underline{0}, \underline{0}, \mathbb{F}_p]$. Thus, in the rest of the proof, we may assume that $|Z| \leq p/2$.

For $1 \leq i \leq n$, we have

$$\sum_{a_i \in \mathbb{F}_p} |X_i \cap (a_i - X_i)| = |X_i|^2, \quad \sum_{b_i \in \mathbb{F}_p} |Y_i \cap (b_i - Y_i)| = |Y_i|^2,$$

which implies that

$$\prod_{i=1}^{n} \left(\sum_{a_i \in \mathbb{F}_p} |X_i \cap (a_i - X_i)|\right)\left(\sum_{b_i \in \mathbb{F}_p} |Y_i \cap (b_i - Y_i)|\right) = \prod_{i=1}^{n} |X_i|^2|Y_i|^2.$$

Therefore we obtain

$$\sum_{\underline{a}, \underline{b} \in \mathbb{F}_p^n} \prod_{i=1}^{n} |X_i \cap (a_i - X_i)||Y_i \cap (b_i - Y_i)| = \prod_{i=1}^{n} |X_i|^2|Y_i|^2. \tag{1}$$

Let N be the number of pairs $(\underline{a}, \underline{b}) \in \mathbb{F}_p^n \times \mathbb{F}_p^n$ such that

$$|Z|^2 \prod_{i=1}^{n} |X_i \cap (a_i - X_i)||Y_i \cap (b_i - Y_i)| > 2p^{n+2}.$$

It follows from Lemma 3.1 that $[\underline{a}, \underline{b}, \mathbb{F}_p] \subseteq B \cdot B$ for such pairs $(\underline{a}, \underline{b})$. Then by equation (1)

$$\left(\prod_{i=1}^{n} |X_i||Y_i|\right) N + 2p^{n+2}(p^{2n} - N) > \left(\prod_{i=1}^{n} |X_i||Y_i|\right)^2,$$

and so

$$N > \frac{\prod_{i=1}^{n} |X_i|^2|Y_i|^2 - 2p^{3n+2}}{\prod_{i=1}^{n} |X_i||Y_i| - 2p^{n+2}}.$$

By the assumption of Theorem 1.2, we have

$$|B| = |Z| \left(\prod_{i=1}^{n} |X_i||Y_i| \right) > |M_n|^{3/4+\varepsilon} = p^{3n/2+3/4+\varepsilon(2n+1)}. \tag{2}$$

Thus when $n > 1/\epsilon$, we have

$$\prod_{i=1}^{n} |X_i||Y_i| > p^{3n/2+7/4},$$

since $|Z| \leq p$.

In other words,

$$N \geq (1 - 2p^{-3/2}) \prod_{i=1}^{n} |X_i||Y_i| = (1 - 2p^{-3/2}) \frac{|B|}{|Z|} \geq \frac{|B|}{p},$$

since $|Z| \leq p/2$. □

4 Proof of Theorem 1.4

Lemma 4.1. *Let Q be a quasifield of order q and let $[\underline{X}, \underline{Y}, Z] = B \subseteq H_n(Q)$ be a brick. For a given $\underline{a} = (a_1, \ldots, a_n)$, $\underline{b} = (b_1, \ldots, b_n) \in Q^n$, suppose that*

$$|Z|^2 \prod_{i=1}^{n} |X_i \cap (a_i - X_i)||Y_i \cap (b_i - Y_i)| > 2q^{n+2},$$

then we have

$$B \cdot B \supseteq [\underline{a}, \underline{b}, Q].$$

Proof. The proof is similar to that of Lemma 3.1, so we leave some details to the reader. Let

$$X' = (X_1 \cap (a_1 - X_1), \ldots, X_n \cap (a_n - X_n)),\ Y' = (Y_1 \cap (b_1 - Y_1), \ldots, Y_n \cap (b_n - Y_n))$$

and $E \subseteq \mathbf{X}$, $F \subseteq \mathbf{Y}$ in $SP_{Q,n}$ where

$$E = X' \times (-Z + \lambda),\ F = \left\{ (\underline{b} - \underline{y}, -z) \colon z \in Z, \underline{y} \in Y' \right\},$$

and $\lambda \in Q$ is arbitrary. Then $e(E, F) > 0$ which implies that there exist $\underline{x} \in X'$, $\underline{y} \in Y'$, and $z, z' \in Z$ such that

$$z + z' + \langle \underline{x}, (\underline{b} - \underline{y}) \rangle = \lambda.$$

This implies that

$$[\underline{a}, \underline{b}, Q] \subseteq B \cdot B.$$

□

The rest of the proof of Theorem 1.4 is identical to that of Theorem 1.2. We need only to show that if $Z \subseteq Q$ and $|Z| > |Q|/2$, then $Z + Z = Q$. However, this follows since the additive structure of Q is a group.

References

[1] N. Alon and J. H. Spencer, *The Probabilistic Method*, 2nd ed., Wiley-Interscience, 2000.

[2] M. Aschbacher, *Finite Group Theory*, Vol. 10. Cambridge University Press, 2000.

[3] A. Brouwer and W. Haemers, *Spectra of Graphs*, Springer, New York, etc., 2012.

[4] P. Diaconis, Threads through group theory, *Character Theory of Finite groups*, *Contemporary Mathematics*, **524** (2010): 33–47.

[5] G. A. Freiman, Addition of finite sets, *Sov. Math. Dokl.* **5** (1964) 1366-1370.

[6] D. Gorenstein, *Finite Groups*, Vol. 301. American Mathematical Soc., 2007.

[7] B. Green and I. Ruzsa, Freiman's theorem in an arbitrary abelian group, *J. Lond. Math. Soc.* **75** (2007), 163-175.

[8] N Hegyvári and F. Hennecart, A note on Freiman models in Heisenberg groups, *Israel J. of Math.* **189** (2012), 397-411.

[9] N. Hegyvári and F. Hennecart, A structure result for bricks in Heisenberg groups, *Journal of Number Theory* **133**(9) (2013): 2999–3006.

[10] T. Pham, M. Tait, C. Timmons, and L. A. Vinh, A Szemerédi-Trotter type theorem, sum-product estimates in finite quasifields, and related results, *J. Combin. Theory Ser. A* **147** (2017) 55-74.

[11] L. A. Vinh, The solvability of norm, bilinear and quadratic equations over finite fields via spectra of graphs, *Forum Mathematicum*, Vol. **26** (2014), No. 1, pp. 141–175.

Appendix

Proof of Lemma 2.3. Let Q be a finite quasifield of order q and let $SP_{Q,n}$ be the bipartite graph with partite sets $\mathbf{X} = \mathbf{Y} = Q^n \times Q$ where $(x_1, \dots, x_n, z_x) \sim (y_1, \dots, y_n, z_y)$ if and only if

$$z_x + z_y = x_1 * y_1 + \cdots + x_n * y_n. \tag{3}$$

First we show that $SP_{Q,n}$ is q^n regular. Let $(x_1, \dots, x_n, z_x)$ be an arbitrary element of $\mathbf{X}$. Choose $y_1, \dots, y_n \in Q$ arbitrarily. Then there is a unique choice for z_y that makes (3) hold, and so the degree of $(x_1, \dots, x_n, z_x)$ is q^n. A similar argument shows the degree of each vertex in $\mathbf{Y}$ is q^n.

Next we show that λ_2 is small. Let M be the adjacency matrix for $SP_{Q,n}$ where the first q^{n+1} rows and columns are indexed by $\mathbf{X}$. We can write

$$M = \begin{pmatrix} 0 & N \\ N^T & 0 \end{pmatrix}$$

where N is the $q^{n+1} \times q^{n+1}$ matrix whose $(x_1, \dots, x_n, x_z)_X \times (y_1, \dots, y_n, y_z)_Y$ entry is 1 if (3) holds and 0 otherwise.

The matrix M^2 counts the number of walks of length 2 between vertices. Since $SP_{Q,n}$ is q^n regular, the diagonal entries of M^2 are all q^n. Since $SP_{Q,n}$ is bipartite, there are no walks of length 2 from a vertex in $\mathbf{X}$ to a vertex in $\mathbf{Y}$. Now let $x = (x_1, \ldots, x_n, x_z)$ and $x' = (x'_1, \ldots, x'_n, x'_z)$ be two distinct vertices in $\mathbf{X}$. To count the walks of length 2 between them is equivalent to counting their common neighbors in $\mathbf{Y}$. That is, we must count solutions $(y_1, \ldots, y_n, z_y)$ to the system of equations

$$x_z + y_z = x_1 * y_1 + \cdots + x_n * y_n \tag{4}$$

and

$$x'_z + y_z = x'_1 * y_1 + \cdots + x'_n * y_n. \tag{5}$$

Case 1: For $i \leq 1 \leq n$ we have $x_i = x'_i$: In this case we must have $x_z \neq x'_z$. Subtracting (4) from (5) shows that the system has no solutions and so x and x' have no common neighbors.

Case 2: There is an i such that $x_i \neq x'_i$: Subtracting (5) from (4) gives

$$x_z - x'_z = x_1 * y_1 + \cdots + x_n * y_n - x'_1 * y_1 - \cdots - x'_n * y_n. \tag{6}$$

There are q^{n-1} choices for $y_1, \ldots, y_{i-1}, y_{i+1}, \ldots y_n$. Since $x_i - x'_i \neq 0$, these choices determine y_i uniquely, which then determines y_z uniquely. Therefore, in this case x and x' have exactly q^{n-1} common neighbors.

A similar argument shows that for $y = (y_1, \ldots, y_n, y_z)$ and $y' = (y'_1, \ldots, y'_n, y'_z)$, then either y and y' have either no common neighbors or exactly q^{n-1} common neighbors.

Now let H be the graph whose vertex set is $\mathbf{X} \cup \mathbf{Y}$ and two vertices are adjacent if and only if they are either both in $\mathbf{X}$ or both in $\mathbf{Y}$, and they have no common neighbors. For this to occur, we must be in Case 1, and therefore we must have either $x_z \neq x'_z$ or $y_z \neq y'_z$ and all of the other coordinates equal. Therefore, this graph is $q-1$ regular, as for each fixed vertex there are exactly $q-1$ vertices with a different last coordinate and the same entries on the first n coordinates. Let E be the adjacency matrix of H and note that since H is $q-1$ regular, all of the eigenvalues of E are at most $q-1$ in absolute value. Let J be the q^{n+1} by q^{n+1} all ones matrix. By the above case analysis, it follows that

$$M^2 = q^{n-1} \begin{pmatrix} J & 0 \\ 0 & J \end{pmatrix} + (q^n - q^{n-1})I - q^{n-1}E \tag{7}$$

Now let v_2 be an eigenvector of M for λ_2. For a set of vertices Z let χ_Z denote the vector which is 1 if a vertex is in Z and 0 otherwise (ie it is the characteristic vector for Z). Note that since $SP_{Q,n}$ is a regular bipartite graph, we have that $\lambda_1 = q^n$ with corresponding eigenvector $\chi_{\mathbf{X}} + \chi_{\mathbf{Y}}$ and $\lambda_n = -q^n$ with corresponding eigenvector $\chi_{\mathbf{X}} - \chi_{\mathbf{Y}}$. Also note that v_2 is perpendicular to both of these eigenvectors and therefore is also perpendicular to both $\chi_{\mathbf{X}}$ and $\chi_{\mathbf{Y}}$. This implies that

$$\begin{pmatrix} J & 0 \\ 0 & J \end{pmatrix} v_2 = 0.$$

Now by (7), we have

$$\lambda_2^2 v_2 = (q^n - q^{n-1})v_2 - q^{n-1}Ev_2.$$

Therefore $q - 1 - \frac{\lambda_2^2}{q^{n-1}}$ is an eigenvalue of E and is therefore at most $q-1$ in absolute value, implying that $\lambda_2 \leq 2^{1/2}q^{n/2}$.

□